Special Topic Course

COMP 7/8992: AI in Cybersecurity (AIsec)

3 Credit Spring 2026

Instructor: Dipankar Dasgupta

Course Description:
Artificial Intelligence (AI) constitutes an umbrella of techniques, and has proven to provide flexible, adaptable solutions to wide variety of security solutions. These techniques typically include Neural Networks, Fuzzy Logic, Evolutionary Computation, Data Mining, Cellular Automata, Immunological Computation, Game Theory, and other computational intelligence models. Over the last 30 years, AI-based approaches were used to build tools for real-time monitoring, malware detection, log analysis, intrusion detection, etc., providing cross-linking solutions to different cyber security applications. This course will cover various cyber-attack landscapes and how AI-guided strategies can be used for defenses. The effectiveness and limitations of pre-trained Generic LLMs in identifying and mitigating emerging cyber threats.

Prerequisites:

Although no prerequisite courses are required, proficiency in computer networking (protocols and communication) and programming concepts is expected, and some prior knowledge of AI/ML techniques is desirable.

Course Details:

Cybersecurity Topics	AI/ML Principles & Tools
Cybersecurity Taxonomy, Intrusion & Anomaly Detection with AI; Malware Threat Detection; Defense-in-Depth; Deep Learning, Neural Networks, Adversarial Machine Learning, Robustness and Security of AI Models, Ethical Implications of AI in Cybersecurity, Legal & Regulatory Frameworks, Privacy Concerns and Data Protection, Bias and Fairness in AI Systems, Hands-on Labs for Implementing AI Security Solutions Future of AI in cybersecurity; Basics of Security in Privacy; Real World Cyber Applications; Use Cases; Common AI security Tools & Their Evaluation; Ethics & Responsible AI, Types of	AI/ML technologies; Understand the role of AI and its significance for cybersecurity. Identify applications and limitations of AI for cybersecurity and the workplace. Students will be able to define ethical considerations, bias/fairness, privacy, and security issues related to AI development and implementation. Define convolutional neuro networks, recurrent neural networks, and generative models/ autoencoders as they relate to AI and effectively use AI tools in developing solutions to demonstrate their

AI & AI Tools; Legal/Risk; Secure Prompt Engineering. Understanding of offensive/ rogue/malicious use of generative AI.	usage. The use of LLMs and Agentic AIs for cyber defense will be discussed.

Evaluation:

The evaluation process will include course-related activities such as paper presentations, assignments, software testing, tests (and quizzes), and a term project to make sure that the students have integrated the material into best practices of AI for cybersecurity.

The final course grade will be based on the following course-related activities with weights for each component as shown below:

Attendance/Discussion	10%
Presentations	10%
Tests/quizzes/Exams	40%
Experiments/Assignments	20%
Final project + proposal	20%

NOTE: 8000-level section students will have to do additional assigned work in each grading category mentioned above.

Grading Scale:

⍰

A+	95.1-100	**B+**	85.1-88	**C+**	76.1-79	**D+**	60.1-66
A	90.1 -95	**B**	82.1-85	**C**	70.1-76	**D**	50 - 60
A-	88.1 -90	**B-**	79.1-82	**C-**	66.1-70	**F**	< 50

Textbook: AI in Cybersecurity. By Leslie F. Sikos (Editor) 1st Edition, Springer 2019.

Reference material:

- AI for Cybersecurity A Handbook of Use Cases. By Peng Liu, et al. Penn State Cyber Security Lab, https://psucybersecuritylab.github.io/book.pdf.Network Security Essentials: Application and Standards (6th edition) by William Stallings. Pearson 2017.
- Advances in User Authentication (Book). Dipankar Dasgupta, Arunava Roy, Abhijit Nag. Publisher: Springer-Verlag, Inc., August 2017.
- Machine learning in cybersecurity: a comprehensive survey by Dasgupta, D., Akhtar, Z. and Sen, S. The Journal of Defense Modeling and Simulation, 19(1), pp.57-106, 2022.
- AI-Powered Ransomware Detection, by Subash Poudyal and Dipankar Dasgupta, 2021.
- Generative AI in Cybersecurity (Springer Briefs in Cybersecurity) by Leslie F. Sikos, 2025.

- Articles from IEEE Symposium Series on Computational Intelligence in Cybersecurity (SSCI-CICS), Organizer: D. Dasgupta 2007-2023.
- Selected readings